HACKER JOURNAL

n. 54 www.hackerjournal.it QUATTORDICINALE ANNO 3 - 1/15 LUGLIO 2004 - SPED. IN ABB. POST. 70% - MILANO

I segreti per scrivere
un COOKIE

2€
NO PUBBLICITÀ
SOLO INFORMAZIONI E ARTICOLI

SKY davvero a prova di PIRATA?

>DECRETO URBANI
ULTIME NEWS

FETICISMO USB

POTENZA SENZA LIMITI
ANCHE CON IL TUO COMPUTER

40054
9 771594 577001

Anno 3 – N. 54
1 Luglio - 15 Luglio 2004

hack·er (hăk'ər)
"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

editoriale

Boss: TheGuilty@hackerjournal.it

I Ragazzi della redazione europea:
Bismark.it, Il Coccia, Gualtiero Tronconi, Marco Bianchi, Edoardo Bracaglia, One4Bus, Barg the Gnoll, Amedeu Bruguès, Gregory Peron
Contents by MDR

Service: Cometa s.a.s.

DTP: Davide "Fo" Colombo

Graphic designer: Dopla Graphic S.r.l.
info@dopla.com

Copertina: Daniele Festa

Publishing company:
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printing:
Roto 3

Distributore:
Parrini & C. S.PA.
00189 Roma - Via Vitorchiano, 81
Tel. 06.33455.1 r.a.
20134 Milano, V.le Forlanini, 23
Tel. 02.75417.1 r.a.

Abbonamenti:
Staff S.r.l.
Via Bodoni, 24
20090 Buccinasco (MI)
Tel. 02.45.70.24.15
Fax 02.45.70.24.34
Lun. - Ven. 9,30/12,30 - 14,30/17,30
abbonamenti@staffonline.biz

Direttore Responsabile: Luca Sprea

Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.

Contro tutti i monopoli, per tutte le libertà

L'informazione vuole essere libera e a parole c'è libertà di informazione. In effetti possiamo parlare tranquillamente. Ma appena prendiamo in mano un oggetto improvvisamente tutto cambia. Se prendiamo in mano un cellulare diventiamo tracciabili. Se mandiamo SMS iniziamo a comportarci da ricchi. Chi è che ride là in fondo? Fatto caso al costo degli SMS, ultimamente? È cresciuto. Caso? Coincidenza? La libertà non ha il listino prezzi.

Se prendiamo in mano un computer collegato a Internet diventiamo tracciabili. D'altronde un computer senza Internet non serve praticamente più a niente. E fin qui andrebbe ancora bene (intanto sosteniamo tutti il progetto Winston Smith, http://www.winstonsmith.info. Serve). Provate a infilare un DVD nel computer. O un CD musicale. Non cominciano a risuonare nelle orecchie parole come Decreto Urbani? E non parliamo di pirateria, per favore. Quello è lo specchietto per gli sciocchi.

La Finanza fa ispezioni presso i privati solo quando questi esagerano, si dice. Sarà. Intanto la legge mette a disposizione gli strumenti per punire anche chi ha regalato il CD alla fidanzata e si è fatto due MP3 che gli piacevano. Non succederà mai che arrivano a casa tua, sento dire. Vero; ma è una verità che arriva dalla statistica, non dalla giustizia. In teoria, chi ha scaricato una canzone (una) via peer-to-peer può vedersi arrivare a casa i finanzieri. Qualcuno obietta che però sono persone ragionevoli. Speriamolo. C'è chi ha già incontrato il vigile urbano sadico che ti dà la multa anche se hai ragione. Poi vai a contestarla e te la tolgono. Intanto perdi le giornate e, nel caso della finanza, il computer.

Ora prendiamo in mano il telecomando. Siamo liberi. Peccato che Sky stia organizzandosi in modo che, con i suoi decoder, sia possibile vedere solo i suoi canali. Tutti gli impianti con codifica SECA2 sono in via di sostituzione, per passare a NDS. Dicono che SECA2 sia stato craccato. Dicono che il passaggio avviene per colpa dei pirati. Intanto è un'ottima scusa per creare una piattaforma di monopolio, e poi si vedrà (pare che neanche NDS sia così sicuro, e nessuna cifratura è invincibile...).

Abbiamo un nemico: i monopoli. Lo Stato è l'unico a poter decidere di inviare SMS gratis a tutti gli italiani e, anche se i provider telefonici sono tre, si muovono come se fossero uno. Le major discografiche e cinematografiche si comportano tutte allo stesso modo, anche se sono relativamente tante. Si chiama cartello, un altro modo di dire monopolio, un po' più mascherato.

Sky sta lavorando per creare un monopolio di fatto. Come Microsoft, come tanti altri nemici della libertà.

Impariamo a riconoscere i monopoli, mascherati o meno, e a combatterli da veri hacker. Con l'arma della conoscenza e della coscienza critica.

theguilty@hackerjournal.it

HACKER JOURNAL: INTASATE LE NOSTRE CASELLE

Diteci cosa ne pensate di HJ, siamo tutti raggiungibili via e-mail, tramite lettera o messo a cavallo... Vogliamo sapere se siete contenti, critici, incazzati o qualunque altra cosa! Appena possiamo rispondiamo a tutti, scrivete!

redazione@hackerjournal.it

La prima rivista hacking italiana

SAREMO DI NUOVO IN EDICOLA GIOVEDÌ 15 LUGLIO!

UN GIORNALE PER TUTTI: SIETE NEWBIE O VERI HACKERS?

Il mondo hack è fatto di alcune cose facili e tante cose difficili. Scrivere di hacking non è invece per nulla facile: ci sono curiosi, lettori alle prime armi (si fa per dire) e smanettoni per i quali il computer non ha segreti. Ogni articolo di Hacker Journal viene allora contrassegnato da un level: NEWBIE (per chi comincia), MIDHACKING (per chi c'è già dentro) e HARDHACKING (per chi mangia pane e worm).

NEWBIE — MID HACKING — HARD HACKING

Impostazioni freeHACKnet

Se già possiedi un account@hackerjournal.it puoi usufruire degli stessi dati di username e password.

Dati per la connessione
Numero telefonico per la connessione: 7020005073

Username: la tua email (nome@hackerjournal.it)

Password: la tua password

Altri servizi
Server SMTP: smtp.hackerjournal.it

Server POP3: pop3.hackerjournal.it

Server NNTP: news.hackerjournal.it
Server FTP: ftp.panservice.it

Assistenza tecnica: info@hackerjournal.it

Ricordiamo che l'e-mail si attiverà quando riceverà il primo messagio... quindi per attivarla basta mandare un e-mail al vostro indirizzo @hackerjournal.it

Pop3 e Smtp da utilizzare per l'e-mail di hackerjournal.it. Se preferisci consultare l'e-mail tramite il tuo client di posta elettronica (Outlook, Eudora, ecc...), ti ricordiamo i seguenti parametri da impostare:

pop: pop3.hackerjournal.it

SMTP: Devi usare i parametri che stai attualmente utilizzando per la tua connessione ad Internet.

Se per esempio utilizzi libero inserisci smtp.libero.it, se usi Tin mail.tin.it e se usi la nostra connessione usa smtp.hackerjournal.it.

Importante: come username devi inserire l'indirizzo di posta completo e non solo il suffisso.

Account di posta elettronica

Impostazioni posta elettronica Internet (POP3)
Tutte le seguenti impostazioni sono necessarie per il funzionamento dell'account di posta elettronica.

Informazioni utente
Nome: Redazione Hacker Journal
Indirizzo posta elettronica: redazione@hackerjournal.

Informazioni server
Server posta in arrivo (POP3): pop3.hackerjournal.it
Server posta in uscita (SMTP): smtp.hackerjournal.it

Informazioni accesso
Nome utente: redazione@hackerjournal.
Password: *************
Memorizza password
Accedi con autenticazione password di protezione (SPA)

Prova impostazioni
Dopo aver immesso le informazioni richieste, è consigliabile provare l'account scegliendo il pulsante in basso. È necessaria la connessione di rete.
Prova impostazioni account ...
Altre impostazioni ...

< Indietro | Avanti > | Annulla

Nuova Password!

Ecco i codici per accedere alla Secret Zone del nostro sito, dove troveremo arretrati, sfondi, informazioni e approfondimenti interessanti. Con alcuni browser, può capitare di dover inserire due volte gli stessi codici. Non fermiamoci al primo tentativo!

USER: nul87

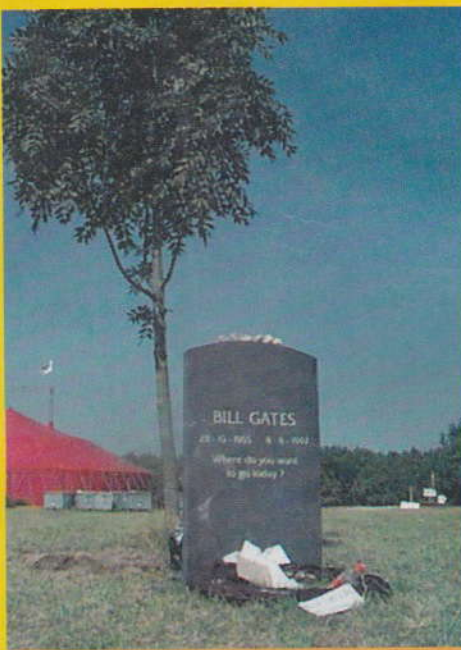
PASS: GGBB

SMEMBRIAMO OGGETTI CON DENTRO... QUALCHE CONTRADDIZIONE

Vorrei scrivere questa mail mosso da quelli che ritengo dei modi sbagliati di affrontare delle faccende:esempio... in un numero scorso (non ricordo quale) viene fatta una critica a microsoft per il fatto che "Grazie alla taglia di quest'ultima" viene catturato in germania l'autore di Sasser... sembra una cosa da far west, è vero ma leggendo ci si rende conto di come quasi si voglia difendere questa persona... un ragazzo si di 18 anni ma che ha creato un bel po' di danni con il suo operato facendo perdere tempo e denaro a migliaia di persone... me compreso... cioè, okay che siamo in internet e tutto è senza regole ma questa persona è un vero delinquente,non si può negare!! I mezzi di informazione hanno reso facile questo purtroppo. Trovo lodevole il fatto di HJ di smembrare qualsiasi argomento che parli di qualche oggetto che contenga differenze di potenziale in qualche sua parte... però trovo sbagliata la posizione che assumete rispetto al mondo che ci circonda. Si cerca (ad es.) in tutti i modi di proteggere il P2P quando ognuno di noi sa benissimo che il 99,99% delle volte che viene usato è per passarsi roba piratata... evviva il condividere ma anche questo è un vero furto... io lo faccio a volte, ma non dico che se tutti vogliono condividere allora è giusto perché mi fa comodo... il fatto di non dare a un autore di qualsiasi cosa niente in cambio del suo lavoro mi dispiace dirlo ma è proprio un furto, anche se non è quel famoso piatto di pasta che, o lo mangio io o lo mangi tu,non si può fare niente purtroppo. Stessa cosa per l'atteggiamento volto a-una-certa-societa-di-redmond-di-cui-non-faro-il-nome-soft... non so perché tutti gli danno addosso per quello che fa (cioé fare affari,non si può dire che Zio Bill non sia un vincente :-(- purtroppo ne sa non si può negare - e continuano a usare windows, boh deve essere il fatto che per natura bisogna sempre e in ogni caso dare addosso alle persone con più influenza di noi.

Tutti dicono Win pieno di bug ma su internet per ogni tre exploit di win ce n'è sicuramente uno per linux... Linus Torvald diceva "Windows continuerà ad essere per linux quello che è sempre stato: un non-problema" della serie: Viva l'open source ma non è alla portata di tutti" Insomma il senso di questa missiva? Occupiamoci di Studiare ciò che ci circonda senza giudicare, che non siamo certo persone in grado di farlo... questo secondo me è un hacker... uno che sa e vuole sapere al massimo di un qualche argomento... poi le sue idee "politiche" su da che parte stare se le fa lui ,non le passa certo ad altri come ogni tanto (perdonatemi :-)) fate un po' voi... del resto gran bella rivista... una (o forse l'unica) delle poche serie in edicola. Le persone che fanno casini per imporre le proprie ideologie non sono certo hackers... sono estremisti del C@$$o. Mi piacerebbe mettere la mia mail lemorragia@yahoo.it per discuterne e vedere quanti mailbombing mi arrivano... giusto per confermare le due righe di sopra. Qua si segue sempre con attenzione

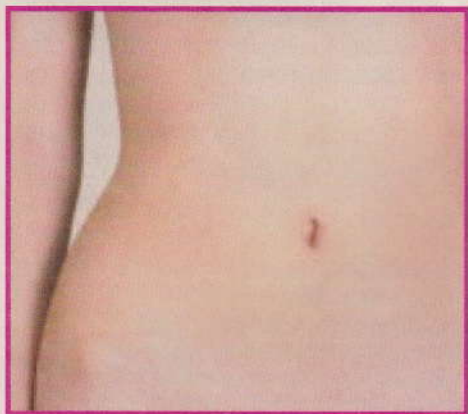
L'Emorragia

Ecco smembrato anche "L'Emorragia" che, secondo noi, ha messo non poca carne al fuoco! Risposte? In linea generale non ne daremo, e lasciamo ai lettori un civile e pacato confronto con le idee di tutti e di ciascuno. Solo due cose: tutti contro Microsoft e zio Bill? Verso la persona, assolutamente nulla. Verso i prodotti che si sono imposti come unica soluzione... stiamo ai fatti. Il 90 % (forse più) del malware in circolazione esiste perché un brodo di coltura ne permette l'esistenza: Windows, per intenderci. Apprezzeremmo molto di più che i "generosi" slanci per frenare il fenomeno e le immense ricchezze di una società con decine di migliaia di dipendenti (per questo Zio Bill andrà comunque in paradiso: c'è chi può sfamarsi anche tramite lui... ;)) fossero indirizzati a costruire sistemi in modo strutturalmente differente, come altri hanno dimostrato di saper fare, e quindi a prova di tentazioni d'attacco. Hai ragione da vendere quando dici che non si può imporre la propria ideologia a nessuno. Ma questo non vuole dire che non si debba commentare nulla. Semplicemente si esprime un proprio parere a fronte di fatti accaduti e di un punto di vista che ciascuno di noi ha acquisito per storia, esperienza, tradizione e chi più ne ha...

Dopodichè la bontà di una posizione (o viceversa la sua assurdità) convincerà anche altri a seguirla (o viceversa a rinnegarla). Quindi: hacking a tutto spiano! Nel senso di studiare, curiosare, conoscere, capire, giudicare (perché no?), ma non imporre. Sarebbe fanatismo.

ESPLOSIONI INTESTINALI!

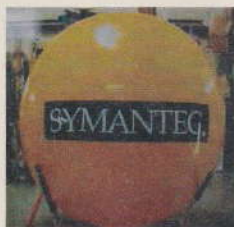
Ciao a tutti!
Ho preso al volo la sfida di Giuliano per i googlewhack con due parole consecutive e questi sono i risultati: "anatra legnosa" "black berlusca" "pioggia acquosa" "rotto gatto" "urbani's show" "decreto assassino" "esplosioni intestinali".
Ok, ho dedicato 15 minuti della mia vita a questo nuovo passatempo. Grazie

Angelo

Sotto con i Googlewhack! Ma non dimentichiamoci anche gli altri motori di ricerca... ;)

SYMANTEC IN-SECURITY?

Carissimi, ho letto con grande soddisfazione il vostro articolo sul Norton Internet fasulla-Security. A questo proposito volevo segnalarvi che l'aggiornamento del 12 maggio 2004 scaricabile col LiveUpdate, manda nel pallone il NIS e il Personal Firewall edizioni del 2002, nel senso che dopo l'update il servizio symproxysvc.exe del Symantec Proxy Service, nel momento in cui decidi sventuratamente di accedere ad Internet, blocca il processore impedendo di fatto la navigazione. La cosa è riportata su diversi forum e, di fatto, sembra che l'unica soluzione sia quella di mettere mano al ripristino configurazione di sistema, giacché la Symantec si limita a consigliare di contattare telefonicamente il servizio clienti. Alcuni utenti addirittura fanno sapere che l'azienda sostiene di non avere in programma il rilascio di patch perché il programma ormai non è più supportato! Considerando che dopo quasi un mese dall'aggiornamento incriminato per poter navigare devo bloccare il firewall (bello tenerlo lì sul desktop, peccato per l'icona un po' spartana) che, strano a dirsi, invece dovrebbe servire a proteggere la stessa navigazione, mi sono posto alcuni interrogativi: che senso ha aver pagato per un programma adesso inutilizzabile? Per non parlare poi di coloro che magari hanno acquistato il servizio di LiveUpdate (io per fortuna formatto il disco fisso almeno due volte all'anno, quindi la cosa non mi tocca), a cosa gli serve? Anche se disinstallano il programma e lo reinstallano poi non potranno nemmeno tenere aggiornato il firewall, rischiando di applicare nuovamente l'aggiornamento incriminato. Domanda maliziosa ma che sorge spontanea dal fondo del cervello: manovra commerciale...?

Daniele – LordFly

Confermiamo: è successo anche ad alcune nostre macchine. Non si può risolvere se non aggiornando alla versione 2004 e sul sito c'è anche scritto che allo scadere dell'abbonamento non verranno più rinnovati quelli delle vecchie versioni: l'unica possibilità è aggiornare il tutto all'ultima realease. Perdendoci circa la metà dell'abbonamento annuale (che ci scade in settembre), abbiamo disinstallato tutto (non semplice nemmeno quello!) e siamo passati immediatamente a ClamWin Antivirus, in licenza GNU e perfettamente funzionante. E per fare contenti i nostri lettori abbiamo deciso di metterlo sul CD di Hackers Magazine che trovate in edicola. E non veniteci a dire che è pubblicità occulta: puro servizio di scaricamento e di tutorial all'uso! ;)

MULTIFORME INGEGNO

Sono riuscito a creare un computer utilizzando una console xbox,un vecchio pentium 100 e un commodore64. Ho creato anche un sistema operativo che ho chiamato Xwhite. Volevo chiedervi se era possibile ricevere i diritti di autore per questa mia creazione.

mstrWhite

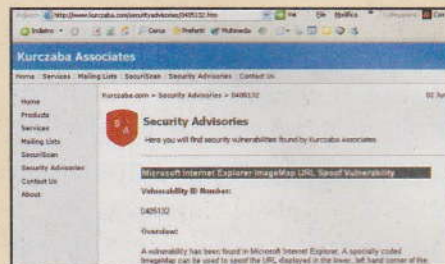
Si, solo se fa anche il caffè ;)
No, non prendertela! Siamo dei giocherelloni! Immaginiamo quanti sforzi e quante ore tu abbia perso sul tuo progetto. Ma rimaniamo interessati e incuriositi: ci vuoi spiegare esattamente cosa intendi per computer, visto che ne hai usati tre diversi per averne uno? Attendiamo maggiori specifiche, più notizie, qualche precisazione...

HOT!

LA GUERRA DI TROJAN

Attacco a tutto campo: le polizie di tutto il mondo sono sulle tracce dei creatori di virus, trojan e worm d'ogni genere. L'ultimo arresto della polizia taiwanese è quello di Wang An-ping, un ingegnere di trent'anni accusato di avere scritto e diffuso Peep, worm che ha infettato i computer dello stesso governo taiwanese.
Lui si difende dicendo che non poteva prevedere la diffusione e il danno, ma ovviamente nessuno gli crede. Anche perché è vero che l'età dell'adolescenza sta elevandosi in tutto il mondo, ma se uno a trent'anni non ha ancora capito alcune cose, forse non è del tutto sano.
Oppure non è del tutto ingenuo. Ed è esattamente per questo che rischia cinque anni di carcere. Non è il solo. In Canada è stato fermato un ragazzo di 16 anni, sospettato di avere scritto il worm Randex. Se lo avesse fatto realmente, anche lui verrebbe accusato di uso fraudolento di computer e danni al sistema informativo della Royal Canadian Mounted Police. Niente su cui scherzare.

MICROSOFT EXPLORER: C'È TRUCCO E C'È INGANNO!

Andate con Internet Explorer all'indirizzo http://www.kurczaba. com/securityadvisories/0405132poc.htm e passate il mouse sopra l'URL www.microsoft.com. In basso a sinistra appare, come sempre, lo stesso indirizzo a cui in teoria sarete reindirizzati. Fate clic e... sorpresa! Vi trovate invece sul sito www.linux.com! Com'è possibile? Ovviamente sfruttando l'ennesima falla di Microsoft Explorer. È stato scoperto che una mappa immagine opportunamente codificata confonde il browser a tal punto da renderlo vulnerabile all'URL spoofing. In sostanza un metodo perfetto per mascherare un reindirizzamento anche all'utente più smaliziato. Provate adesso con Opera e con qualunque altro browser: come passate sopra il link, in basso a sinistra viene svelato il trucco e quindi non potete cascarci.

HARRY POTTER SOTTO STRETTA SORVEGLIANZA

Nei cinema britannici si vedono in sala loschi figuri che girano con monoculari per la visione notturna, in grado di rivelare qualunque tentativo di pirataggio del film. Le attuali telecamere digitali, di dimensioni piccolissime e prestazioni eccezionali, permettono infatti di registrare praticamente al buio le scene sullo schermo, utilizzate poi dai pirati per creare e diffondere sul mercato i DVD dei film in prima visione.
Di bassa qualità, ovviamente, ma non così tanto da evitare che migliaia di sprovveduti li acquistino.

OCCHIO ALLE BANCONOTE FALSE

Un telefonino con fotocamera integrata, un filtro sotto forma di carta di credito e chiunque, perfino alla debole luce di una lampadina di cortesia in auto, può controllare se una banconota è falsa oppure no. Lo propone un'azienda italiana, L.A. Torino srl (http://www.moneycontrolsystem. com/). È uno speciale filtro da tenere davanti all'obiettivo della fotocamera, integrato in una scheda delle dimensioni di una carta telefonica. Uno scatto, e della banconota appaiono solo le apposite bande di sicurezza che ci dicono se è veramente uscita dal conio ufficiale.

FOTO ANCHE DAL CORDLESS

Siete in camera da letto e volete inviare una bella foto al vostro fidanzato? Il telefono cordless Gigaset SL740 di Siemens integra una fotocamera che potrete scaricare su Internet, per condividere gli scatti con chi volete.
È il primo telefono fisso che ha questa capacità, mentre la privacy... la privacy? Cos'è la privacy? Chi ha parlato di privacy?

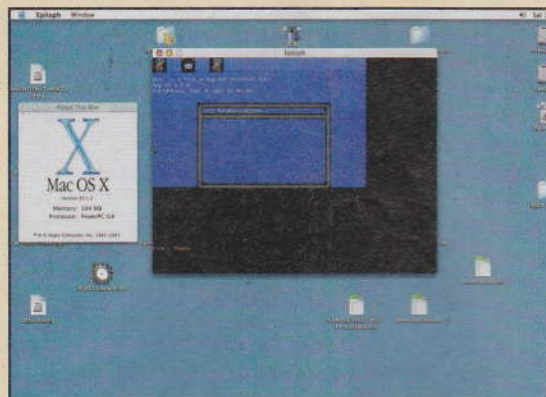
VIETNAM? NO GRAZIE.

Dibattere contro un governo comunista porta a spiacevoli conseguenze: sta emergendo solo ora all'attenzione del resto del mondo che in Vietnam, da marzo di quest'anno, per accedere agli Internet Café si è obbligati a esibire dei documenti di identificazione e la traccia di ogni navigazione deve essere conservata per almeno 30 giorni, sui server locali. Nguyen Minh Vinh, funzionario di polizia cha ha collaborato alla stesura delle nuove norme, ha specificato anche che i proprietari degli Internet Cafè sono obbligati a conteggiare il tempo speso online da ciascun utente e mantenere firewall e software di protezione sempre aggiornati, pena 3.200 dollari di multa e processo conseguente. Negli ultimi due anni sono aumentati a dismisura i cyber dissidenti che usano la rete per appoggiare la protesta contro il governo comunista. Nelle scorse settimane, Nguyen Vu Binh, un giornalista di una rivista considerata vicina al regime, ha dovuto difendersi contro una sentenza che gli appioppava la bellezza di 7 anni di prigione, essendo stato accusato di spionaggio per aver inviato via email un articolo che criticava il suo governo.

WI-FI IS HOT, SECURITY IS NOT

Da Los Angeles a San Francisco in Toyota 4Runner, alla caccia di hot spot WiFi a cui attaccarsi. Ne hanno scovati tremilaseicento, all'ottanta percento dei quali è stato possibile collegarsi perché privi delle più elementari norme di sicurezza. Se andiamo avanti così pare evidente che il fenomeno WiFi porterà alla possibilità di collegamento a partire da qualunque punto del globo, ma in totale mancanza di controllo di "chi fa che cosa e come". Un progresso di libertà o una minaccia alle reti interne di milioni di persone? Ardua risposta. Attendiamo notizie italiane di war-driver italiani: chi sa, parli.

PATCH SULLA PATCH PER APPLE

Una patch di sicurezza che chiude le falle di una precedente patch per lo stesso problema. Una volta tanto non stiamo parlando di Windows, ma di MacOSX, che finalmente ora sembra sicurissimo e a prova di attacco. All'utente l'incombenza di approvare ogni qual volta viene montata l'immagine di un disco o viene lanciata per la prima volta un'applicazione. Solo così la potenziale backdoor del sistema operativo può essere chiusa, perlomeno a detta di Apple. La società che aveva avvertito il problema non si pronuncia ancora e attende una più profonda analisi per affermare che il buco è stato definitivamente chiuso. Attendiamo anche noi...

HOT!

LADRI DI RAME BLOCCANO INTERNET

La vittima principale è stato il portale di Libero, ma ne ha risentito anche il nostro sito: per sei ore, mercoledì 9 giugno nel nord Italia è andato down il traffico Internet, perché l'effetto ruspa non si è fatto sentire solo a Porta Romana in Milano, dove dentro un tombino un cavo a fibra ottica è stato reciso e bruciato. Questa volta però i lavori stradali non c'entrano niente. Sono stati dei ladri di cavi di rame che hanno pensato bene di portare via dei pezzi di cavo dell'alta tensione, rivendibili a buon prezzo ai rigattieri, e che nella foga (e nell'ignoranza) hanno scambiato un cavo a fibra ottica per un rivestimento di un filo di rame. Le bruciature sono state la conseguenza di un principio di incendio innescatosi per l'alta tensione. Perfino nel sud Italia l'effetto domino sul flusso dei dati si è fatto sentire e sia a Roma, sia a Napoli alcuni server hanno cessato di funzionare. Altro che attentato! Se basta così poco a mettere in ginocchio i backbone nostrani, siamo a posto.

OLIMPIADI SENZA WI-FI

Ai giochi olimpici saranno attivi 10 mila personal computer, 500 portatili, 450 server Unix con Solaris a bordo, perché Sun è sponsor dei giochi e 400 server Windows. Ma niente Wi-Fi. Il cablaggio senza fili è stato considerato poco sicuro dai responsabili dei giochi olimpici di Atene. Quindi anche quest'anno il tutto sarà cablato come in passato, con costi altissimi, ma con maggiore sicurezza rispetto a possibili intrusioni. Perlomeno così dicono i responsabili dell'informatica olimpionica. Per il CIO una minaccia potrebbe venire, senti senti, dagli hacker... Vale una pernacchia olimpionica.

SKY CERCA RIPARO dagli attacchi

Non avrai altri canali oltre ai nostri: ***Sky*** *è passata all'attacco,* ***ma viene attaccata!***

Voci? Dritte? Trucchi? Chiamatele come volete, ma diciamo subito che non risponderemo alle richieste di dove e quando. Di fatto negli ultimi tempi sul web sono apparse pagine, poi repentinamente scomparse, proprio in concomitanza con 290 arresti della Guardia di Finanza in provincia di Agrigento, relativi alla possibilità di vedere i programmi di Sky da parte di molti, avendo però un solo abbonamento.
Chi ha orecchie per intendere…

Il Seca2, lo standard attuale usato dalle pay-TV è così meno sicuro di quanto ci volevano far credere.

Un opportuno uso del software giusto e pare proprio che si riesca a insinuarsi nelle pieghe del super sicuro (ma chi mai lo è veramente?) standard adottato dal potente colosso di Murdoch. Un'occhiata al sito http://www.la-cafetera.com/seca2.htm è solo l'inizio per un approfondimento di tutto quello che non vi possiamo dire, perché comunque teniamo a rispettare la legalità, per quanto generi, a volte, delle ingiustizie. Che non si fanno attendere da parte di Sky stessa che sta correndo ai ripari, mettendo sicuramente nei guai i pirati delle card e i guardoni a sbafo, ma che con la scusa della pirateria in atto di fatto blinda e monopolizza un intero settore.

al SECA2!

Non sarà più lo stesso: gli attacchi a Seca2 costringono Sky a cambiare tutto. Ma diventa soffocante monopolio.

La libertà digitale ne viene perfino compromessa, al punto che i produttori di decoder stanno cercando di mettere con le spalle al muro la stessa Sky, aggrappandosi all'Autorità per la concorrenza e citando Sky per abuso di potere. L'accusa: Sky sta buttando fuori dal mercato i costruttori di decoder alternativi.

"Qualora un utente fosse già abbonato a Sky - ha dichiarato l'azienda produttrice di decoder Jepssen - e in possesso di un decoder common interface oppure decidesse in futuro di acquistarlo e sottoscrivere l'abbonamento, sarebbe, di fatto e in ogni caso, costretto a utilizzare unicamente quello fornito da Sky Italia, poiché non sono disponibili sul mercato moduli Cam NDS per Sky Italia".

Sky ha deciso: cambia tutto. Cambia lo standard, che da Seca2 passa al più sicuro (fino a prova contraria, visto che qualche ricerca in ambienti israeliani sta ponendo alcuni fondati dubbi in proposito) standard NDS. E cambia anche i decoder: che verranno sostituiti a casa di tutti gli utenti abbonati a Sky.

Così, con la scusa di voler combattere le card pirata, Sky (www.skytv.it) entro la fine del 2004 Sky trasmetterà utilizzando soltanto il sistema di codifica NDS e abbandonerà il sistema di codifica SECA. Attivando il monopolio di fatto: senza decoder Sky, niente programmi Sky.

Ma non solo! La programmazione Sky aumenta di canali propri e vengono buttati fuori canali meno... ortodossi, ma certamente liberi di stare sul mercato. Come Superpippa o Play TV, particolari e di settore certamente, ma altrettanto legittimi, che sono stati eliminati dai canali veicolati da Sky. Che, nella situazione italiana della TV satellitare, significa la certezza di scomparire quasi totalmente. Da qui anche le azioni dei singoli gestori contro Sky, per ora cadute in un nulla di fatto.

L'Autorità garante della concorrenza e del mercato (www.agcm.it) sta studiando il caso. Nel frattempo tra gli utenti serpeggia una nuova paura di libertà persa e soffocante monopolio in arrivo. Tra i proprietari di decoder acquistati c'è chi inizia la protesta con tanto di disdetta all'abbonamento Sky e chi grida ad un nuovo attentato alle libertà digitali.

Uccisi i canali sgraditi: fine certa per alcuni gestori

E ADESSO COME MI COLLEGO A SKY?

I CASI SONO DUE:

1) SONO UN ABBONATO SKY CON UN DECODER GOLD BOX A NOLEGGIO

Mi viene fornita da Sky una smart card NDS oppure un decoder e una smart card NDS, in modo gratuito.

Nel caso il mio decoder sia aggiornabile via satellite, Sky invierà a casa una smart card NDS con tutte le istruzioni per procedere all'aggiornamento automatico del decoder.

Nel caso il mio decoder non sia aggiornabile via satellite, Sky invierà a casa un nuovo decoder e una smart card NDS. Il decoder Gold Box e la relativa smart card li potrò utilizzare per la ricezione dei canali digitali in chiaro via satellite.

2) SONO UN ABBONATO SKY CON UN DECODER GOLD BOX DI PROPRIETÀ

Sky mi fornirà un decoder e una smart card NDS in comodato d'uso gratuito. L' attuale decoder e la relativa smart card posso utilizzarli per la ricezione dei canali digitali in chiaro via satellite.

USB Senza

Nelle porte dei PC di oggi si può inserire proprio di tutto, e non solo strumenti da hacker! Ecco cosa abbiamo trovato ...

La nascita di USB, negli anni Novanta, è stata accompagnata da una certa indifferenza. Poi Apple l'ha messa nei suoi Mac e il suo uso è improvvisamente esploso. Oggi non c'è computer che ne sia privo e soprattutto ci sono accessori per tutti i gusti, dall'hackeristico al completamente inutile ma divertente. Primo fra tutti: il coltellino svizzero. Chi può farne a meno, se smanetta con i computer, o con qualsiasi altra cosa? Ebbene non c'è esemplare completo senza i suoi bei 64 o 128MB di memoria Flash USB (più puntatore laser).

Per non dare nell'occhio, per fare lo scherzone all'amico o anche solo per facilitarsi il lavoro, esiste uno switch USB a pedale. Delcom Engineering, lo stesso produttore, mette a disposizione anche segnalatori luminosi, display digitali e lampade che cambiano colore secondo lo stato del computer. Spetta a noi pensarne un uso intelligente.

Sorregge il foglio e lo illumina. Niente di meglio per trascrivere al volo un documento con il portatile!

Urgenze, Sicurezze, Baluardi

USB può anche essere un ricevitore GPS fatto apposta per portatili. Anche in mezzo al deserto sappiamo dove siamo, sempre ammesso di avere

BARRIERE

UTENSILI SPECIALMENTE BRILLANTI

Il coltellino svizzero, 89,40 euro più IVA: http://www. icebergtechnology.com. Lo switch USB a pedale, 29 dollari, http://www.delcom-eng.com/ products_USBFSW.asp.
Il sensore GPS per portatili, 89 dollari, a http://store.l-f-l.com. Il diffusore di essenze profumate, 38 dollari, a http://usb.brando.com.hk/usbaromapot.php.
La FlyLight per illuminare la tastiera al buio 19,99 dollari (25/30 euro in negozio), http://www.kensington.com/html/1176.html. Anche in variante-leggio ClipNGlow, 24,99 dollari, http://www. kensington.com/ html/1413.html.
Lo ionizzatore/purificatore d'aria di Delta Global Crew, 20 dollari, http://usb.brando. com.hk/usbinoizer.php. E quello di ThinkGeek, a 29,99 dollari, http:// www.thinkgeek.com/gadgets/electronic/68ce/zoom/. Il ventilatore FlyFan di Kensington, 9,99 dollari, a http://www.kensington.com/html/ 1265.html.
Il massaggiatore da 18 dollari, a http:// usb.brando.com.hk/usbmassageball.php.

batterie… per lavori al buio, invece, dove non ci sono altre fonti di luce (o quando non vogliamo rivelarci!), è indispensabile la FlyLight Kensington, discreta e perfetta per illuminare solo e soltanto la tastiera (parliamo per esperienza). Per la massima sicurezza, aiuta disporre di uno scanner di impronte digitali come lo U.are.U 4000 di DigitalPersona (http://www.digitalpersona.com/products/sensor.html). Oppure viaggiare con i dati cruciali nascosti nell'…orologio, come il DiskGo di Edge (se ne trovano un po' dappertutto, dai cento euro in su) o i modelli LaCie da 128 e 256MB (http://www.lacie.com/it/). Non è l'impianto intramuscolare per passare i controlli degli aeroporti, ma supererà un controllo distratto.

Un Sano Benessere

Vogliamo parlare di comfort, invece? A volte per programmare o smanettare bisogna essere concentrati al massimo e avere l'atmosfera adeguata. Tanto per cominciare, se dobbiamo trascrivere qualcosa di stampato è difficile avere meglio di un ClipNGlow Kensington. Ideale per i portatili, è una FlyLight con un mezzo un leggio, che illumina il documento intanto che lo regge. Negli ambienti di ufficio o dove l'aria non è il massimo si può attaccare all'USB uno ionizzatore, che filtra l'aria e la purifica. O anche un piccolo bruciatore per diffondere nell'aria aromi di oli essenziali.

Per l'estate un FlyFan Kensington consente di affrontare il caldo. Mica solo il PC deve avere la sua ventola! E quando abbiamo finito di lavorare al computer… spalle indolenzite? Sindrome da tunnel carpale? Niente paura. C'è persino il massaggiatore!

▲ *E se serve, ecco un lettore di impronte digitali.*

Terminata questa veloce panoramica, che avrebbe potuto essere dieci volte più lunga e non stiamo scherzando, rimane una domanda: ma chi fabbricherà un hub abbastanza capace da collegare tutta questa roba? :-)

Reed Wright
reedwright@mail.inet.it

Aria fresca, un bel massaggio e un po' di luce, tutto rigorosamente USB!

CIFRARE CON LE

La cifratura probabilistica è un campo assai complicato ma promettente per la sicurezza dei dati e delle informazioni

Un esempio interessante e atipico di cifratura è quella probabilistica, in cui un messaggio viene cifrato in un certo numero di testi in cifra possibili. Questo approccio è diverso da tutti gli altri sistemi di cifratura, che sono deterministici; ovvero da un singolo testo in chiaro deriva un singolo testo in cifra). In generale la sicurezza della cifratura probabilistica è legata alla difficoltà di risoluzione di un problema assai difficile, come per esempio ricavare i due numeri primi che hanno generato un numero intero molto grande, o procedimenti ancora più astrusi, come quello basato sul residuo quadratico.

La cifratura probabilistica consente di fare cosette interessanti in completa sicurezza, come dimostrano i prossimi due esempi, banali quanto basta.

IL MISTERO DEL RESIDUO QUADRATICO

La cifratura scivola spesso nella matematica di alto livello. la cifratura probabilistica si allaccia alla nozione di residuo quadratico. Nello studio delle equazioni diofantine e nello studio dei numeri primi è importante sapere se un numero intero a è il quadrato di un intero modulo p. Se è così, a è un residuo quadratico. Per esempio, 4^2 modulo 9 = 7 (cioè 7 è il resto della divisione per 9 dell'elevazione al quadrato. Possiamo dire in questo esempio che 7 è un residuo quadratico modulo 9.

Testa e croce via telefono

Come si fa a giocare a testa e croce, giusto per avere il gioco più semplice possibile, se i giocatori non si possono vedere e non possono controllare che cosa ha tirato l'altro? Diciamo che Alberto e Barbara vogliono giocare. Si mettono d'accordo sul fatto che testa e croce hanno le stesse probabilità di uscire, dopo di che:

PROBABILITÀ

- **Alberto sceglie i parametri** del suo sistema di cifratura e li tiene segreti.
- **Alberto manda a Barbara** una versione cifrata di testa e una versione cifrata di croce.
- **Barbara sceglie uno dei due messaggi** e lo rimanda ad Alberto.
- **Alberto rivela la sua chiave segreta** e tutti e due possono verificare il risultato. Di fatto, è stata tirata una moneta in modo assolutamente casuale.

Controllo del partner

Non è per gelosia, ma per sicurezza. Sto veramente parlando con chi penso o qualcuno sta facendo ingegneria sociale alle nostre spalle?

Supponiamo che Angie e Bart abbiano condiviso a suo tempo una Chiave Segreta. Ora Angie vuole inviare un messaggio a Bart e vuole essere certa che sia proprio lui.

- **Angie genera un Valore Casuale** e lo invia a Bart.
- **Bart cifra il Valore Casuale** con la Chiave Segreta e lo rimanda, cifrato, ad Angie.
- **Angie intanto cifra anche lei Valore Casuale** e Chiave Segreta.
- **Se il valore da lei ottenuto** e quello che le arriva da Bart sono uguali, vuol dire che Bart è proprio lui (o che qualcuno ha rubato la Chiave Segreta, ma questo è un altro problema).

Se un aggressore sta spiando il dialogo tra Angie e Bart può intercettare Valore Casuale e cifratura, ma non ha idea della Chiave Segreta.

Allo stesso modo, Andrea e Billie possono creare e scambiarsi chiavi sicure utilizzando il metodo di distribuzione delle chiavi di Diffie-Ellman:

- **Si parlano,** anche in pubblico, e concordano un Numero Primo e un Generatore del gruppo moltiplicativo Z[**Numero Primo]**.
- **Ognuno dei due** sceglie la sua chiave privata.
- **Andrea calcola Generatore** elevato alla sua chiave segreta, modulo Numero Primo, e manda il risultato a Billie.
- **Billie calcola Generatore elevato** alla sua chiave segreta, modulo Numero Primo, e manda il risultato ad Andrea.
- **Andrea e Billie calcolano la Chiave Segreta** elevando il Generatore a ciò che gli arriva, modulo p.

Un intruso può ascoltare tutte le conversazioni in corso, ma non potrà ragionevolmente scoprire la Chiave Segreta.

Per sviscerare completamente l'argomento si dovrebbe scendere molto più in dettaglio, ma le cose si fanno rapidamente troppo matematiche per una rivista come la nostra! Ma chi si è incuriosito ora ne sa abbastanza per approfondire…

Nyarlathotep
nyarlathotep@hackerjournal.it

```
      1.
      1.3
      2.13
      3.213
      5.0213
     11.33213
     15.220213
     25.0303213
     41.34350213
    102.235433213
    133.3553520213
    222.25525003213
    333.425113050213
    522.3414514133213
   1203.53241532220213
   2005.521025203303213
   3012.5013420051350213
   4321.13223301152433213
  10501.520351315510520213
  14132.5005451554442003213
  23221.13124155541030050213
  35031.515102555313431133213
  54345.4544342551523445220213
```

▲ *Generare numeri veramente casuali è difficile. Soprattutto non è semplice accorgersi se sono casuali davvero!*

▲ *L'ideogramma che significa fortuna. Parlando di cifratura probabilistica e numeri casuali sembra appropriato!*

LA PALUDE DEI GRUPPI MOLTIPLICATIVI

Quando parliamo di generatori e gruppi moltiplicativi, funziona così. Quando un numero è primo (cioè si divide solo per 1 e per se stesso), il gruppo moltiplicativo degli interi modulo p è ciclico e quindi possiede un generatore, che ha periodo pari al numero primo meno uno.
In concreto. Prendiamo un primo, per esempio 13. Ora guardiamo le potenze di 2 modulo 13:

2 4 8 3 6 12 11 9 5 10 7 1

Dopo di che il ciclo si ripete. Questo gruppo moltiplicativo contiene dodici elementi, uno in meno di tredici, e il suo generatore è appunto 2.

Webbit ATTERRA

Per chi fosse atterrato su questo pianeta solo ora, da quattro anni a Padova si tiene Webbit (http://webb.it). È una fiera informatica ma anche un grande Lan party e una preziosa area di scambio di conoscenze tra aziende, organizzazioni libere, sviluppatori open source e qualsiasi tipo di iniziativa non allineata all'ovvio.

Webbit fa il suo ingresso in Milano!

Bene: Webbit arriverà anche a Bari (nel prossimo ottobre). E intanto, il 3 e il 4 giugno, è sbarcato a Milano presso i padiglioni della Fiera.

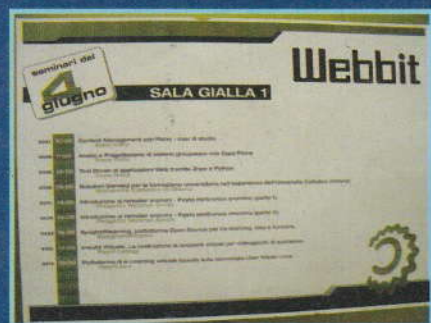
Non è ancora il "vero" Webbit, con la gente che dorme lì o meglio passa la notte alla Lan, i server spontanei sui quali scambiare file di ogni natura, le maratone di programmazione di gruppo, i contest grafici e i Nutella party. Il Webbit propriamente detto in edizione meneghina è previsto per il 2005, se quest'anno l'organizzazione sarà rimasta soddisfatta, e le premesse ci sono tutte. A Milano è infatti arrivato lo scambio di conoscenza, ossia i seminari. Molte delle organizzazioni presenti a Padova si sono ripresentate a Milano con gli stessi contenuti o oppure rinnovati di poco. L'afflusso di gente non può essere lo stesso dell'ambiente padovano, con gli stand aziendali e l'attrattiva della LAN nonstop. Ma le persone interessate ai seminari si sono rivelate in buon numero e l'atmosfera era più che sufficientemente animata. Molta gente si è ritrovata a Milano dopo essersi incontrata al Webbit originale e si è verificato nuovamente quel cortocircuito tra detentori della conoscenza e persone decise a migliorarsi che è il vero succo della manifestazione.

▲ *Grande pubblico e attenzione per uno dei seminari su Zope.*

In preparazione all'invasione prevista nel 2005, arrivano le avanguardie dell'informatica che non dorme mai

A MILANO

Sikurezza e Winston Smith

Privacy, sicurezza, crittografia delle infrastrutture e delle reti wireless sono state solo alcune delle certificazioni che, dopo i successi di Padova, sono state riproposte a Milano, dalle proposte di Sikurezza.org al progetto Winston Smith (http://www.winstonsmith.info), una delle prime realizzazioni della privacy totale che può essere ottenuta con le tecnologie crittografiche esistenti anche se più o meno nessuno lo dice chiaramente, tranne le riviste come questa. Winston Smith è una personalità virtuale, dal nome del protagonista del libro "1984" di George Orwell, che si comporta come un normale utente della rete: pubblica un sito, manda e riceve posta, gestisce una mailing list, ma tutto in maniera assolutamente anonima, riuscendo a conservare perfettamente intatta la propria privacy.

▲ *Questo nutrito calendario era solo una minima parte del programma complessivo. A Webbit c'è un sacco da imparare.*

Tra gli altri seminari in onda a Milano abbiamo visto tanta attenzione per la sicurezza ma anche per l'open source in generale, con tematiche quali gli strumenti open per la comunicazione, l'uso avanzato del sistema di gestione dei contenuti Zope, il calcolo di massa, Linux, il linguaggio di scripting Python e anche un sano seminario indirizzato allo sviluppo di Content Management System in linguaggio PHP.

Tra le cose che non erano da perdere per nessuna ragione spiccavano il percorso di certificazione Understanding The Twenty Most Critical Internet Security Vulnerabilities, con nozioni molto interessanti sulla privacy del wireless e sul filtraggio della posta spazzatura, e Hacking della firma digitale e attacco ai contenuti della smartcard. Alcune casistiche. Tenuto dal mitico Kobaiashi di Sikurezza.org, è uno dei seminari andati in overbooking, talmente prenotato che si rischiava di non avere posti liberi in sala.

Insomma, il Webbit di Milano non poteva avere la stessa eco di quello originale... per stavolta. Nel frattempo, appuntamento a Bari per il prossimo ottobre!

Michele Campovecchio
michele_c@hackerjournal.it

Un WORM per

Incredibile: cosa c'entra il padre di "Great Worm" con Yahoo!? Scopriamolo assieme

Robert Tappan Morris Jr. figlio di uno dei maggiori responsabili dell'NCSC, il centro per la sicurezza informatica dell'NSA (National Security Agency), si confronta presto con la cruda realtà dell'hacking leggendo articoli e scoprendo alcune note particolarmente tecniche del padre. Lo stesso poliziotto informatico avvia il figlio al mondo dei computer. I prestigiosi studi ad Harvard lo avvicinano ancor di più all'informatica e all'applicazione delle conoscenze circa il mondo Internet e Unix. Ha la possibilità, piuttosto rara negli anni '80, di possedere un computer tutto suo, ma soprattutto di poter accedere a una serie di strumenti top secret: racconta di come abbia messo le mani su Enigma, la misteriosa quanto importante macchina cifratrice della Seconda Guerra Mondiale. La passione per l'hacking è di difficile attribuzione temporale. Lo stesso Morris Jr. non ricorda bene quando sentì la "voce che lo chiamava all'hacking". È indubbio, comunque, che egli esprimesse potenzialità enormi seduto a quel computer: racconta di come abbia ottenuto diritti di root addirittura nella rete dei Bell Labs. Proprio questo exploit, che a suo avviso fu di una semplicità disarmante, lo avvicinò ad approfondire meglio le problematiche relative alla sicurezza informatica. L'ingresso alla Cornell University lo indusse in seguito a cercare di capire il funzionamento della struttura Internet e di cogliere le debolezze di Unix. Decide così di mostrare al mondo, in via molto pratica, come ARPANET e Internet in generale poggiasse su basi non proprio solide, come invece si voleva far credere.
Fu così che nell'ottobre 1988 iniziò un progetto personale volto ad attaccare quanti più computer connessi alla rete mondiale senza creare danni ai sistemi.

Internet era quasi tutta qui: Arpanet all'inizio del 1977

Lo scopo era creare un worm capace di autoreplicarsi in maniera veloce e in tutte le direzioni.

Nasce il Great Worm

Robert è conscio di trovarsi di fronte a un problema semplice: costruire un piccolo programma che, nascondendosi, deve replicarsi sfruttando quelle che sono le debolezze di Unix. Le scoperte che gli sono utili sono essenzialmente due: la distribuzione BSD presenta qualche problema con finger (il demone che risponde alle domande che arrivano dalla rete) e sendmail (il sistema che gestisce la posta elettronica). Il worm, nel suo bootstrap, si installa sulla macchina bersaglio e poi carica sulla stessa macchina il worm vero e proprio che va alla ricerca di password. Tali password gli sono utili per poter accedere a più postazioni possibili e nello stesso tempo deve potersi replicare via Internet tramite sendmail e senza essere scoperto.
Programmato un sistema del genere, Morris aggiunge il codice letale, quello per cui la creatura sfugge al controllo del creatore. La funzionalità in questione è il "modus infectandi" del worm: non un replicarsi in maniera raziocinante, ma secondo una cieca casualità. Praticamente le macchine, anche se già infettate, saturano la propria capacità di elaborazione per rispondere al replicarsi del worm.
Questo inconveniente è del tutto sottovalutato da Morris Jr. che decide, nella notte del 2 novembre 1988, di far debuttare la sua invenzione. Seimila computer vengono attaccati, i sistemi della NASA subiscono infiltrazioni da parte del Great Worm, l'aeronautica degli Stati Uniti registra la sua presenza nelle proprie macchine, ARPANET per alcune ore collassa. È il panico totale. Per mettere fine all'azione del worm si mobilitano l'intero MIT e la University of Carolina. Dopo pochi giorni soltanto da Berkeley sembrano giungere opportune contromisure, seppure temporanee. Lo stesso Morris, via BBS, resosi conto dei danni provocati dalla sua creatura, invia messaggi con

FARSI CONOSCERE

consigli per bloccare il worm. Attorno all'argomento si scatenano i media con il tono di una apocalisse informatica.

Giustizia, fama... e ricchezza

Non passa molto tempo prima che RTM venga arrestato.
La condanna potrebbe essere durissima: 5 anni di carcere e 250mila dollari di multa; invece, dopo una campagna mediatica pro-Morris, la pena risulterà essere nettamente più mite. Il suo exploit è di importanza notevole sotto l'aspetto giudiziario: è la prima condanna per la violazione del CFAA, la legge contro la criminalità informatica. Inoltre, dopo tale hack, il governo statunitense organizza il CERT con lo scopo di intervenire e contrastare incidenti informatici di tale portata. Come in ogni vicenda sfuggita al controllo dell'autorità qualcuno cerca perfino di tingerla di mistero, attribuendone la vera paternità al gruppo Legion of Doom: i servizi segreti si mobilitano, ma il tutto si sfalderà come neve al sole. Uscito di galera, ad aspettare Robert ci sono, oltre che i familiari e gli amici, anche 49 milioni di dollari: la cifra per la quale qualche annno dopo venderà, all'ormai famosa Yahoo!, un'azienda di nome Viaweb fondata per commercializzare un software di creazione dei siti di e-commerce. Il Lab for Computer Science del MIT gli offre un posto che non può rifiutare: cattedra di insegnamento.
L'unica cosa che gli è stata chiesta – si racconta – è che non si faccia venire in mente una nuova idea di come mostrare al mondo quanto debole è l'infrastruttura Internet.

United States District Court

Northern District of New York

U.S. v. Robert Tappan Morris

Case Number 89-CR-139

Defendant's Attorney: Thomas A. Guidoboni, Esq.

THE DEFENDANT was found guilty on Count 1 of the Indictment after a plea of not guilty.

Accordingly, the defendant is adjudged guilty of such count(s), which involve the following offenses:
18 USC, Sec. 1030 (a)(5) Intentional access of Federal interest computers without authorization thereby preventing authorized access and causing a loss in excess of $1,000.00

The defendant is sentenced as provided in pages 2 through 7 of this Judgment. The sentence is Imposed pursuant to the Sentencing Reform Act of 1984.
The mandatory special assessment is included in the portion of this Judgment that imposes a fine.

Date of Imposition of Sentence: May 4th, 1990

[signed] Howard G. Munson
USDJ/NDNY
May 16, 1990

[Page 2 of 7]

PROBATION

The defendant is hereby placed on probation for a term of three years.

While on probation, the defendant shall not commit another Federal, state, or local crime and shall comply with the standard conditions that have been adopted by this court (set forth on the following page). If this Judgment imposes a fine or a restitution obligation, it shall be a condition of probation that the defendant pay any such fine or restitution. The defendant shall comply with the following additional conditions:

▲ *Tre anni, multa e recupero in comunità sociale: come diventare famosi.*

Alone Sparrow
kikocorsentino@email.it

Un IDEA per CIFRARE

Come è fatto l'algoritmo talmente brevettato che lo trattano praticamente come se fosse free

IDEA (International Data Encryption Algorithm) è un algoritmo piuttosto interessante, perché in alcuni punti ricorda una funzione di hash non reversibile più che un cifrario a blocchi. È interessante anche il fatto che eviti di usare tabelle di lookup o S-box.

L'algoritmo usa 52 sottochiavi, ognuna di 16 bit. Cifra in otto fasi. Prima di ogni fase e al termine dell'ultima fase vengono usate quattro chiavi; altre due chiavi vengono usate durante ogni fase.

Il blocco di testo in chiaro viene diviso in quattro parti, ognuna da 16 bit. L'algoritmo parte da due valori di 16 bit per arrivare a un risultato, sempre di 16 bit, mediante tre operazioni: addizione (con riporti, modulo 65.536), XOR e moltiplicazione. Questa avviene in modo particolare; in IDEA un blocco di 16 bit tutti a zero rappresenta, per convenzione, il numero 65.536.

In questo modo la moltiplicazione può avvenire in modulo 65.537, che è un numero primo, ed è possibile la reversibilità dell'operazione.

BREVETTATO CON IL CERVELLO

Si parla spesso della questione della brevettabilità del software e dei relativi abusi compiuti dalle aziende, che complicano la vita di chi sviluppa software libero. Prendano esempio da Ascom (http://www.ascom.ch), azienda svizzera che ha creato l'algoritmo IDEA. Lo ha brevettato, ma concede praticamente sempre il permesso di usarlo gratuitamente per uso non commerciale. Non sempre è questione di regole; conta anche l'intelligenza.

Descrizione di IDEA

Chiamiamo i quattro pezzi di testo A, B, C e D e le 52 sottochiavi da C1 a C52. Prima della prima fase avvengono le seguenti operazioni:

A XOR Y
C XOR Y
B XOR X
D XOR X

Klartext: Blöcke fester Länge (64 Bit)

Beschreibung von IDEA

Bild 2: Der IDEA-Algorithmus.

Scambiare B e C

Tutto questo va ripetuto altre sette volte (otto volte in totale), usando le chiavi da C7 a C12 per la seconda fase, fino a quando l'ultima fase usa le chiavi da C43 a C48. Alla fine dell'ottava e ultima fase non si scambiano B e C.

Infine:

A * C49
B + C50
C + C51
D * C52

A * C1
B + C2
C + C3
D * C4

La prima fase è questa:

A XOR C (chiamiamo il risultato X)
B XOR D (chiamiamo il risultato Y)
X * C5 (prendiamo il risultato come nuovo valore di X)
X + Y (prendiamo il risultato come nuovo valore di Y)
Y * C6 (prendiamo il risultato come nuovo valore di Y)
X +Y (prendiamo il risultato come nuovo valore di X)

Decifrazione

Il trucco per la decifrazione si basa sul fatto che in ogni fase A XOR C non cambia il valore ove A e C siano stati XORati con lo stesso valore, quale che sia. Lo stesso vale per B e D.

Le prime quattro chiavi di decifrazione (CD) sono:

CD1 = 1/C49 (inverso, modulo 65.537)
CD2 = - C50 (complemento a 2)
CD3 = - C51
CD4 = 1/C52

Poi si ripete otto volte quanto segue, aggiungendo ogni volta 6 al numero di ogni chiave di decifrazione e togliendo 6 al numero di ogni chiave di cifratura:

CD5 = C47
CD6 = C48

CD7 = 1/C43
CD8 = - C44
CD9 = - C45
CD10 = 1/C46

Generazione delle sottochiavi

La chiave a 128 bit di IDEA è composta dalle prime otto sottochiavi, da C1 fino a C8. Le otto sottochiavi successive si ottengono nello stesso modo, dopo uno shift circolare a sinistra di 25 bit, e la procedura si ripete fino a quando non sono state derivate tutte le sottochiavi di cifratura.

Ne0k0n
ne0k0n@hackerjournal.it

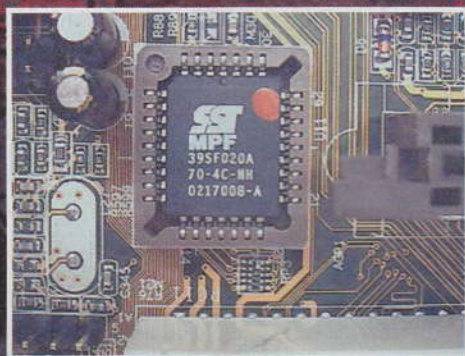
Quanto è robusta l'IDEA

L'unica vera debolezza possibile di IDEA consiste nella procedura di generazione delle sottochiavi, che è regolare e quindi passibile di attacco. Tuttavia tutti i test condotti sulla cifratura di IDEA hanno dato buoni risultati e la comunità considera questo algoritmo altamente sicuro. Questo è dovuto anche all'ingegnoso uso delle operazioni di addizione, moltiplicazione e XOR per evitare l'uso di tabelle di lookup e S-box.

All'ATTACCO

Con tutti i rischi e pericoli che comporta, la modifica del BIOS può dare grandi soddisfazioni

Tutti sappiamo che il BIOS è essenziale al funzionamento del nostro computer. Lì dentro ci sono le istruzioni che permettono alla nostra macchina di avviarsi, caricare tutto quello che serve per pilotare i diversi circuiti della scheda madre e così via. Un sacco di BIOS sono più o meno standardizzati nel kernel, e poi vengono personalizzati dai singoli produttori di schede madri che ci aggiungono tutto quello che a loro serve. La maggior parte degli attuali BIOS è modulare: un po' di codice è messo dal produttore, un po' dall'assemblatore della scheda madre e un po'... da noi. Il BIOS è memorizzato su una memoria ROM flash, che quindi può essere riscritta. La dimensione di questa memoria va, all'incirca, dai 128 ai 512 kbyte nei casi più complicati. I dati sono registrati serialmente e sono compattati, per cui non c'è da meravigliarsi se i driver impacchettati lì dentro hanno poi una dimensione ben maggiore.

Per esempio, se abbiamo una scheda che comprende anche i chip che pilotano la rete locale, al BIOS va aggiunto il driver specifico per quella circuiteria. La lan-on-mainboard, abbreviata lom, per funzionare ha infatti bisogno di software che venga caricato fino dalla fase del PXE (si pronuncia "pixie") ovvero il Pre-Boot Execution Environment, che prepara tutta la circuiteria al boot vero e proprio. Spesso tra i file che vengono dati sul CD che normalmente correda le schede madri, ci sono anche questi driver. A volte invece no, ma forse li possiamo cercare su Internet. Purtroppo capita anche che i file ci siano, ma non siano stati caricati nel BIOS e che quindi dobbiamo farlo noi. Se analizziamo il BIOS con un editore esadecimale, possiamo individuare parecchi componenti software anche compressi.
Se è così, alla fine della memoria riservata al BIOS viene messo un loader, che si incarica di far partire la macchina ed estrarre tutti i pezzi compressi mettendoli in RAM.

▲ *Un chip che contiene il BIOS, su una moderna scheda a 64 bit.*

Metterci le mani

Mettere le mani sul BIOS è certamente molto rischioso: se sbagliamo qualcosa il problema può bloccare la partenza stessa del computer e quindi dobbiamo stare sempre attenti ad avere, da qualche parte, una copia esatta del contenuto originario del BIOS, che possiamo tenere di backup e usare in caso di necessità per ripristinare il tutto. Queste sono operazioni da veri esperti.

In rete ci sono parecchi strumenti, naturalmente, che ci possono aiutare in queste faccende. Awdflash.exe, cbrom.exe e cbrom6.exe sono alcuni di

del BIOS

e risolvere casi complessi. Vale la pena cominciare a introdurci nell'ambiente ...

questi. Però non possiamo dare una ricetta unica di utilizzo, perché naturalmente dipende dalla scheda madre che si possiede. Per le schede AMI con l'AMI BIOS esiste uno strumento apposito: amibcp.exe.

Dopo che è stata salvata un'immagine completa del BIOS presente (per esempio come file bios.bin) o che ci siamo accertati che esista un file analogo sul sito del produttore della stessa scheda madre, il comando

```
cbrom bios.bin /d
```

mostra quanto spazio è rimasto per introdurre nuovo codice.
Se la ROM Flash del BIOS contiene codice compresso, il programma cbrom è in grado di comprimere e salvare in formato compresso il codice che vorremo aggiungere. Più o meno, per esempio, è necessario uno spazio libero compreso tra 8 e 20 kbyte per farci stare un driver di rete (ovviamente dipende dal driver).
Nel caso ci si accorgesse che non c'è abbastanza spazio libero di memoria, si possono togliere dei driver non essenziali o di componenti che non si usano. Per esempio, il logo del produttore può essere un buon elemento da eliminare senza che nessuno ne senta la mancanza. Viene in aiuto, in questo caso,
un comando come

```
cbrom bios.bin /[pci|ncr|logo|isa] release.
```

La linea di comando

```
cbrom bios.bin /[pci|isa] bootimg.rom [0000:0]
```

aggiunge invece il codice compilato alla bios.bootimg.rom, cosa che altrimenti dovremmo fare programmando un'altra EEPROM. Se per esempio stiamo installando la scheda di rete, possiamo usare entrambe le opzioni PCI o ISA, secondo il tipo. Con una scheda ISA dobbiamo dire a cbrom da quale locazione della RAM va estratto il codice, nel momento del boot. La differenza tra fare questa aggiunta a questo livello invece che da un floppy (come il floppy di emergenza che in genere si tiene da parte) è essenzialmente quella che in questo caso noi stiamo agendo _prima_ che il sistema abbia attivato la possibilità di leggere dal driver del floppy! Cosa che, infatti, non è sempre detto che sia possibile. E il codice introdotto verrà eseguito sempre prima che lo stesso floppy sia disponibile, se c'è.

COME RECUPERARE IL BIOS SE QUALCOSA VA STORTO

Tutte le operazioni fatte o che si faranno, sia chiaro, sono a nostro rischio e pericolo. Metterci le mani, lo ripetiamo, può causare l'impossibilità di riaccendere normalmente il computer. Necessita una scheda madre identica con un BIOS funzionante.

1) bootstrappare con un floppy DOS contenente lo strumento software di riscrittura della flash rom del BIOS;
2) scrivere il contenuto del BIOS della nostra scheda madre in un file;
3) rimuovere (okkio!) il chip del BIOS _senza spegnere la macchina_! E' più facile se il chip è su zoccolo...;
4) inserire il chip dell'altra scheda madre dello stesso tipo in cui abbiamo inserito il codice non funzionante;
5) far girare nuovamente l'utility che installa il BIOS nel chip appena inserito;
6) se abbiamo un altro chip identico possiamo anche ripetere il passo 5 per avere un chip di backup;
7) ri-bootstrappare la macchina che dovrebbe ripartire...

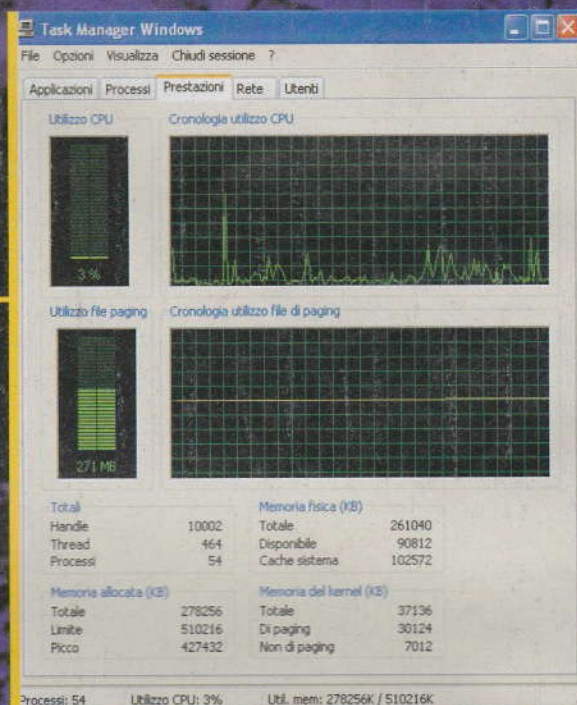
Diventiamo un PEZZO DI UN COMPUTER

Raggiungiamo potenze inimmaginabili, eppure è solo un puzzle fatto di tanti piccoli pezzettini. Internet è anche questo: contribuire personalmente alle ricerche più avanzate

La maggior parte del tempo la CPU si annoia. Al lavoro!

Grazie a Internet mettere insieme la potenza di tutti i computer del mondo è teoricamente possibile. Non è nemmeno necessario che siano tutti collegati nello stesso momento: basta che ciascuno svolga bene un piccolo lavoro che gli viene assegnato e poi ne restituisca il risultato. Tutti i risultati possono essere raccolti e uniti da un computer appena più potente, fino a ottenere risposte impensabili anche se impiegassimo la più potente macchina di calcolo attualmente esistente. La bellezza di questo sistema è che il nostro piccolo computer può svolgere il suo compito sfruttando solamente i tempi morti della CPU, quindi tutti i momenti in cui il microprocessore non deve effettuare delle operazioni particolari. E sono la maggior parte! Se guardiamo il Task Manager di Windows (Ctrl-Alt-Del) alla voce Prestazioni > Utilizzo CPU ci accorgiamo subito che i momenti in cui il micro lavora tanto sono veramente pochissimi. Per la gran parte del tempo, se stiamo facendo cose normali come scrivere, navigare, ascoltare musica, eccetera, la CPU entra in un ciclo di attesa da cui esce solamente in caso di reale necessità. Fantastico. Se decidiamo di partecipare a un progetto di elaborazione distribuita, la nostra CPU sarà finalmente impegnata a tempo pieno. Innanzitutto per noi se serve, ma soprattutto per l'elaborazione in tutti i tempi morti disponibili, in modo del tutto trasparente e senza che ce ne accorgiamo o che le prestazioni ne risentano.

Partecipiamo anche noi

I progetti che sfruttano questo concetto non sono moltissimi, ma sono tutti interessanti. Probabilmente il più famoso è SETI, Search for Extraterrestrial Intelligence, alla ricerca di segnali potenzialmente inviabili da intelligenze extraterrestri. Sulla terra riceviamo infatti miliardi di segnali dallo spazio, generati da chissadove e finora attribuiti a radiogalassie ed altri oggetti emettitori di frequenze varie. Ma chi ci dice che tra questi non ci siano anche dei segnali con un preciso significato, di qualcuno che ha tentato o sta tentando di mettersi in comunicazione con noi? Non c'è computer che tenga: anche i più grandi supercomputer del mondo non possono stare dietro all'enorme massa di dati che bisognerebbe analizzare. Ecco, allora, l'idea: spezzare il problema in tanti piccoli (si fa per dire) frammenti e distribuire l'analisi dei frammenti a tanti piccoli computer: i nostri. Seti@home è un client che si scarica dall'indirizzo http://setiathome.ssl.berkeley.edu/ e che senza interferire

The Amiga RC5 Team Effort

GIGANTESCO

▲ *Per la sfida sono organizzati centinaia di gruppi. Che utilizzano i computer più diversi o riutilizzano computer obsoleti. Più si è, più probabilità ci sono di vincere!*

con le nostre cose, si collega nei momenti di pausa e analizza segnali dei radiotelescopi. È anche possibile associarsi a team specifici i cui risultati sono conteggiati assieme, così che si attiva una specie di gara tra diversi gruppi e tra singoli, con segnalazioni speciali di chi ha contribuito di più e meglio al progetto.

Folding@Home è un progetto della Stanford University. In parole semplici, anche se le cose sono decisamente complicate, il progetto cerca di capire al meglio come sono prodotte le singole proteine che hanno a che fare con le funzioni del nostro organismo e che sono sintetizzate sotto gli ordini dei geni che possediamo. Se si riuscisse a produrre molecole sintetiche fatte nello stesso modo, si potrebbero correggere i vari disastri che la natura ogni tanto ci propina, come il morbo di Alzheimer, la fibrosi cistica, il morbo della "mucca pazza" e altri. Il compito del nostro computer sarà proprio quello di cercare di capire, per un gruppo specifico di molecole, quali possono essere i metodi di ricombinazione, o qualcosa di simile.

Genome@Home è il progetto fratello di Folding@Home e cerca di comparare i nostri geni con altri presenti in natura, per tentare di capire a cosa servono. Analogo, con un altro client e organizzato da bioinformatics.ca, è il progetto Distribuited Folding presso http://www.blueprint.org/.

RC5 (http://distributed.net/) è un progetto sfida nato da alcuni appassionati per cercare di scardinare i codici crittografici della RSA. In 212 giorni, distribuendo il client ai PC collegati a Internet, è stato scardinata la chiave a 56 bit, con un numero di tentativi pari a 7 miliardi di chiavi al secondo. Qualunque computer singolo non avrebbe potuto nemmeno provarci. Dopo 1.757 giorni, il 14 luglio 2002 è stata scardinata anche la chiave a 72 bit. 331.252 i partecipanti alla gara. È in corso la sfida per i 72 bit e i premi sono anche ricchi: 1.000 dollari è il premio per chi riesce a trovare la chiave crittografica, 6.000 dollari se è un'organizzazione no-profit. Più ci si collega, più si hanno possibilità di vincere. Altri sistemi crittografici nel frattempo scardinati con lo stesso metodo sono stati DES e CSC. Tutti stroncati nel giro di poche ore.

Ecco dove qualcuno ha raccolto la sfida e ha installato il client. Se ne contano centinaia di migliaia.

Http://climateprediction.net/ è la casa di un altro progetto che funziona più o meno così. Sappiamo tutti che le attuali previsioni del tempo fanno cilecca da tutti i punti di vista. Qui su carica sul proprio PC un sistema che simula una situazione climatica in qualche parte del mondo, la sviluppa e ne invia i risultati all'elaborazione centrale. Più si tiene il client attivo, più anni climatici vengono elaborati e, probabilmente, in futuro avremo la possibilità di creare un modello globale del clima capace di dirci se domenica possiamo andare al mare: senza sorprese.

Il Rothberg Institute For Childhood Diseases è un'organizzazione senza fini di lucro che ha creato il client utile all'elaborazione distribuita di una ricerca contro i tumori e una forma di sclerosi nei bambini.
I progetti sono quindi due e due sono i client scaricabili dall'indirizzo: http://teamdiscovery.net/

Morte allo SPAM a COLPI di REGEX

I distributori di posta-spazzatura sono sempre più subdoli e aggressivi. Ci tocca dotarci di strumenti sempre più potenti. Come le espressioni regolari!

La frase che appare in grande in queste pagine è l'ultimissimo spam che ci è arrivato. Sembra proprio vero. Ma il link non porta da nessuna parte, e l'allegato non è esattamente simpatico. Veri bastardi, questi spammer! Ma possiamo essere più furbi di loro, se impariamo a dominare le espressioni regolari per catturare le parti di messaggio che si ripetono ma non sono facili da descrivere.

A caccia di Viagra

Ecco alcune regex di esempio buone per catturare alcuni spam tipici.

```
(?i)v\W?i\W?a\W?g\W?r\W?a
```

Questa regex individua la parola Viagra, scritta in qualunque forma (anche vIaGrA, per dire). L'operatore \W identifica un qualunque carattere non alfanumerico (diverso da lettere e numeri), per cui potremmo catturare anche Via$gra. Il punto interrogativo che segue \W indica che il carattere non alfanumerico è opzionale.

```
(?i)p\W?e\W?n\W?i\W?s
```

Beh... se la prima regex trovava Viagra, che cosa potrebbe trovare la seconda?

```
(?i)<\s*img[^>]+(?:low)?src\s*=\s*
(?:'|")\s*http:
```

Qui il gioco si fa duro. Questa espressione regolare riconosce qualunque tag <img> in HTML contenente un URL. Sono tag noiosi, perché sembra che mostrino semplici immagini, ma in realtà vanno a prendere roba (chissà di che tipo) su Internet. Per la cronaca, \s indica un cosiddetto whitespace character come spazi, tabulatori, ritorni a capo, tutto ciò che è un carattere ma non si vede. L'asterisco significa riconosci il simbolo precedente in sequenze lunghe da zero a infinito, ossia \s* *vuol dire individua tutti i whitespace character consecutivi presenti in questo punto della sequenza.*

```
(?i)http://\S*\.biz
```

Questa espressione regolare cattura tutti gli URL che finiscono in .biz (è biz-zarro, ma molti indirizzi collegati

Ciao!
Francesca ha visitato il nostro sito, cartolina.it e ha creato una cartolina virtuale per te! Per vederla devi fare click sul link sottostante:
http://cartolina.it/asp.viewcard index4g345a
Attenzione, la cartolina sarà visibile sui nostri server per 2 giorni e poi verrà rimossa automaticamente. (allegato: link.cartoline.it.viewcard.index.4g345a.pif)

allo spam hanno questo suffisso). È interessante notare la sequenza \. Il punto, nelle regex, indica *qualsiasi carattere;* ma noi vogliamo che in questo caso indichi solamente il carattere punto. Il backslash (\) prima del punto avvia una cosiddetta *sequenza di escape* che toglie al punto che segue qualsiasi significato aggiunto.

Da questi semplici esempi si può partire per costruire regex anche molto precise, che intercettino lo spam come missili Patriot.

Barg the Gnoll
gnoll@hackerjournal.it

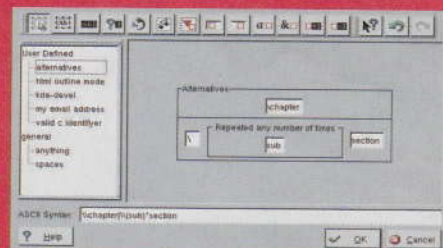
LE INTESTAZIONI DI FRANCESCA

Ecco lo header della finta cartolina virtuale della finta Francesca:

Return-Path: <tcomunic@hotmail.com>
Original-Recipient: rfc822;pippo@peppo.it
Received: from mail.tiscalinet.it (82.48.224.188) by mail-1.tiscali.it (7.1.016.11)
id 40C6A46500002F92 for pippo@peppo.it; Wed, 16 Jun 2004 00:34:12 +0200
Message-ID: <x993630924.9458938330773566945@lnvunjdsv>
From: Francesca <tcomunic@hotmail.com>
To: <pippo@peppo.it>
Subject: Ti e stata inviata una Cartolina Virtuale!
Date: mer, 16 giu 2004
MIME-Version: 1.0
Content-Type: multipart/mixed;
boundary="--=_Part_18357_8384177.7257053348412"
X-Priority: 3
Microsoft Outlook Express 5.00.2314.1300

È lavorando su questa parte del messaggio, normalmente non visibile, che le regex possono dare un grande aiuto.

MA 'STE REGEX?

Le espressioni regolari, o regex, individuano schemi di testo complessi e permettono ricerche molto più sofisticate del semplice comando Trova di un programma tipico. Su HJ ne abbiamo parlato più volte e continueremo a farlo.
Gli esempi qui riportati sono in sintassi Python, ma si possono scrivere praticamente in qualsiasi linguaggio. Per saperne di più si può approfondire su siti come http://www.corsolinux .it/testi/perl/analog/le_espressioni_regolari.jsp. Programmi per trattare regex si trovano per esempio a http://weitz.de/regex-coach/ (Windows), http://txt2regex.sourceforge.net (Linux) e http://www.toolusersoft.com/ (Mac OS X).

CUCINARE

Piccoli e insidiosi pezzettini di software, si installano senza nemmeno che ce ne accorgiamo. Buoni o cattivi che siano, come vengono usati alle nostre spalle? E come si creano?

Ecco le risposte

Che abbiamo già sentito parlare dei cookie è sicuro, anche se l'argomento in questione è un po' ambiguo e risulta difficoltoso stabilire se i "biscotti" (il significato della parola cookie) sono buoni o cattivi. Cerchiamo di capire perché.

Un cookie è un file di testo che può racchiudere fino a 4 Kb di dati, che risiede dal lato client (sul disco rigido dell'utente) e a cui il browser accede esclusivamente se il sito da remoto lo chiede. In pratica è il "contenitore" sul lato client delle informazioni memorizzate dalle applicazioni sul lato server.

Per vedere se il browser dell'utente che visita il sito ha l'abilitazione ad accettare i cookie oppure no, si sfrutta la variabile HTTP_COOKIE.
Ecco il codice per metterlo in pratica:

```
<%
if request. ServerVariables
("HTTP_COOKIE") <> "" then
 response.write "I cookies sono
abilitati"
else
 response.write "ATTENTO! cookies
non sono stati abilitati"
end if
%>
```

Creiamo un cookie

La sua creazione, per tutte le tecnologie come l'ASP e il PHP, deve avvenire assolutamente prima di qualsiasi tag HTML. Ecco la creazione di un cookie in ASP:

```
<%
response.Cookies("nome_cookie")
= "Hacker Journal"
%>

<h1>
```

i COOKIE

```
<% response.write "Il cookie creato contiene : " &
response.write(request.Cookies("nome_cookie"))
%>
</h1>
```

Siccome non abbiamo impostato una data di scadenza, non sarà permanente e quindi non verrà prodotto alcun file e "scadrà" alla chiusura della connessione. Per dare un tempo di vita preciso al cookie è necessario che utilizziamo quest'altro script:

```
<%
 response.Cookies("nome_cookie") =
"Hacker Journal"
 response.Cookies("nome_cookie").Expires = DateAdd("d", 14, Date)
%>
```

In questo modo il cookie scadrà fra due settimane, perché non facciamo altro che addizionare 14 giorni alla data corrente. Ma attenzione: il cookie scadrà al termine della giornata specificata in base alla locazione del server.

Gestione visite - Microsoft Internet Explorer

Benvenuto!

Questa è E' la tua prima visita e oggi è il 11:56:55 21/12/2003

Elimina il cookie

Ecco il risultato della nostra prima visita a schermo

▲ Possiamo controllare, per esempio se l'utente è sbarcato sul nostro sito per la prima volta

Modificare il cookie

Creato il cookie, per modificarlo basta ristabilire il testo che dovrà contenere, e il nostro "biscotto" sarà automaticamente aggiornato:

```
<%
 response.Cookies("nome_cookie")
= "Hacker Journal - rivista hacking"
 response.write "Il contenuto modificato è : " &
response.write(request.Cookies("nome_cookie"))
%>
```

```
<%
 response.Cookies("nome_cookie")
= ""
%>
```

E ora: PHP!

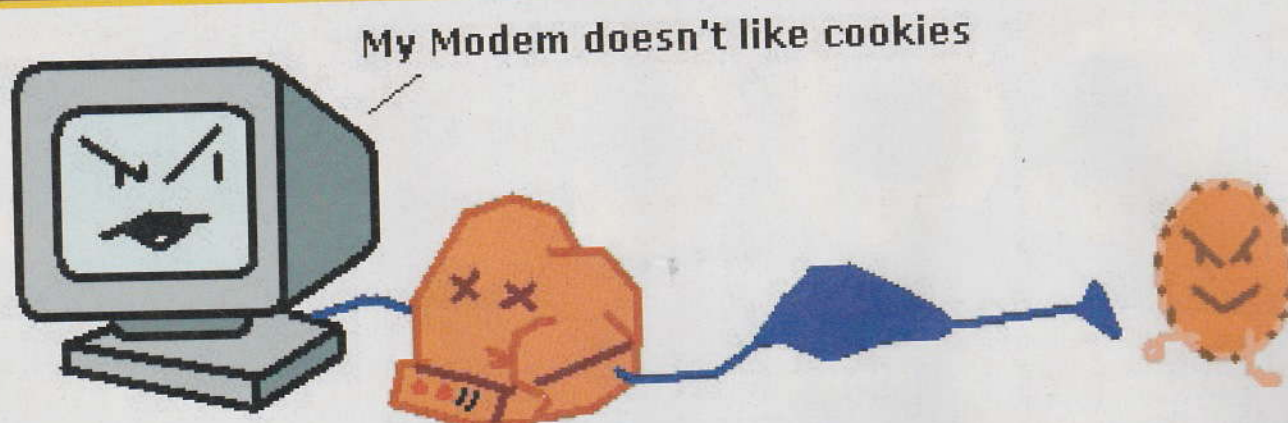
Tutte le operazioni di scrittura, modifica e eliminazione avvengono se impieghiamo la sola funzione setcookie(). Come per l'ASP, dobbiamo invocarla prima di ogni altro codice presente nella pagina Web.

Ecco invece l'output dopo la nostra prima visita

▲ Quando l'utente torna sulle nostre pagine, prendiamo le decisioni che vogliamo.

Eliminare il cookie

È molto più semplice di quanto possiamo immaginare: è sufficiente che assegniamo al cookie una stringa vuota in questo modo:

La funzione prevede due argomenti obbligatori: il nome e il suo valore testuale.
Se per esempio vogliamo salvare la data dell'ultima visita di un utente al nostro sito:

```
<?
setcookie("nome_cookie", time());
?>
```

Impostato il cookie, il valore può essere facilmente modificato richiamando la stessa funzione e cambiando i valori da assegnare. Ma ora vediamo come mostrarne il contenuto sullo schermo:

```
<?
setcookie("nome_cookie", time());
echo "La tua ultima visita è avvenuta il: ".$nome_cookie);
?>
```

Per cancellare il cookie non facciamo altro che assegnargli un valore nullo:

```
<?
setcookie("nome_cookie", "" );
?>
```

Un esempio di progetto

Ora che abbiamo in mano la capacità di gestire i cookie, creiamo passo passo una pagina dinamica in PHP per visualizzare l'ultima visita di un utente, gestendo i due casi:

- prima visita
- ulteriore visita

Se si tratta della prima visita da parte dell'utente, allora creiamo il cookie per la prima volta.
Se invece il visitatore c'era già stato e quindi il cookie era già esistente, basterà che lo visualizziamo.

Ecco lo script del progetto:

```
<?
i                                    f
(isset($HTTP_COOKIE_VARS["nome_c
ookie"])) {

   $benvenuto = "Bentornato!";
        $info =  "La tua ulteriore
visita ed è avvenuta il: ";
        $visita = $nome_cookie;

}else {

    setcookie("nome_cookie",
date("H:i:s d/m/Y"));
        $benvenuto = "Benvenuto!";
        $info = "E' la tua prima visi-
ta e oggi è il ";
        $visita= date("H:i:s d/m/Y");
}
?>
<html>
<head>
<title>Gestione visite</title>
</head>
<h1><?=$benvenuto?></h1>
<p>
Questa è <b><?=$info?><?=$visi-
ta?></b>
</p>
<p>
<a href="cancella.php">Elimina</a>
il cookie
</p>
</html>
```

Già dalle prime righe del nostro progetto impariamo un'altra cosa: l'if iniziale controlla l'esistenza o meno del cookie che a noi interessa e, se esiste, modifica il contenuto delle variabili utilizzate in seguito, utilizzando una volta sola l'output a schermo. Se poi non fosse presente in cache, viene automaticamente creato. Abbiamo anche inserito un link a [cancella.php] che riportiamo qui sotto e che permette l'immediata eliminazione del cookie.

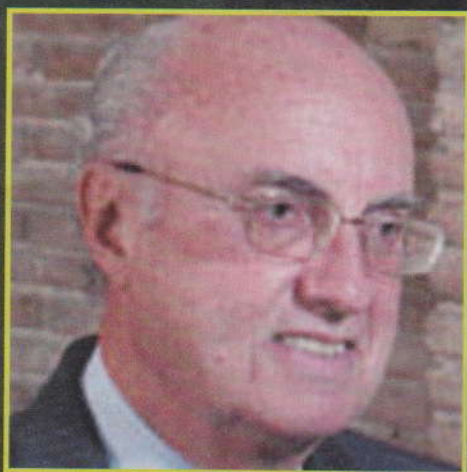
```
<?
 setcookie("nome_cookie","");
 header("location:index.php");
?>
```

Potrebbero starci delle migliorie grafiche, per non dire dell'inclusione di altre proprietà dei cookie (tempo di permanenza e la creazione di molteplici cookie con ruoli diversi), ma questo lo lasciamo alle nostre esplorazioni personali.

Come possiamo ben vedere, molte e altre ancora sono le azioni che i siti, che magari visitiamo con regolarità, possono compiere facendo uso dei cookie. Disabilitarli completamente non sarebbe opportuno perché spesso perderemmo funzionalità, per esempio come accade per il forum di HJ, ma non sono comunque da sottovalutare le possibili conseguenze di eventuali cookie spioni e maligni.

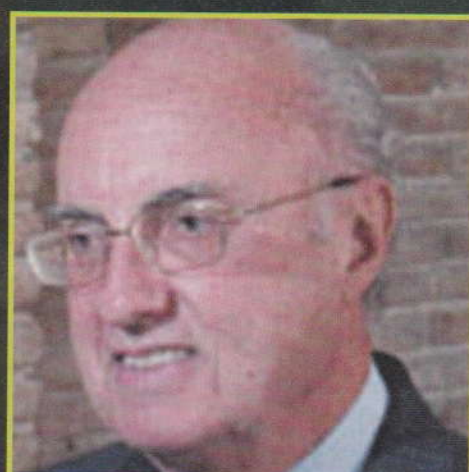
Michele "SoNiK©" Bruseghin
sonik@devpoint.it

Denuncia bomba: LEGGE URBANI CONTRO URBANI!

Della serie: chi la fa l'aspetti! Il sito web del Ministero per i Beni e le Attività Culturali è fuorilegge, secondo l'esposto di un deputato europeo radicale

La legge Urbani dice che si deve mettere sui siti web un avviso che affermi che si è a posto nei confronti delle norme riguardanti il diritto d'autore. Cosa di meglio che andare a vedere se chi ha fatto la legge l'ha fatta anche rispettare sul suo sito? E così è scattata la denuncia da parte di Marco Cappato, un deputato europeo radicale che ha preso avvocato, consulente, penna e fogli e ha consegnato alla Polizia amministrativa e postale un esposto per violazione della legge, da parte del sito dello stesso Ministero di Urbani!

Dalla dichiarazione di Cappato di metà giugno leggiamo: "In questo momento praticamente tutti i siti web potrebbero essere in violazione della Legge Urbani, perfino quello del Ministro che ha voluto la legge. Non è chiaro peraltro l'ambito di applicazione di questo "idoneo avviso", che forse si trasformerà in un "bollino virtuale" con il regolamento tecnico e l'intervento della SIAE. Forse dovrà applicarsi a tutta le rete Internet, svelando così l'assurdità di una pretesa legislativa praticamente inattuabile e giuridicamente risibile. Forse invece riguarderà solo gli operatori italiani, che allora rimarranno ingiustamente discriminati rispetto agli stranieri privi di simili incombenze.[...]".

Pazzesco! E non è l'unico segnale che questa legge è stata fatta senza, evidentemente, avere approfondito bene le conseguenze anche per altri settori dell'informatica.

Per esempio, chi produce software in Italia dovrà sobbarcarsi spese e burocrazia per adeguarsi alle norme. Il software è un'opera dell'ingegno - e ci mancherebbe che non lo fosse! - e quindi per essere distribuito via web, cosa che sappiamo tutti è ormai normale, deve sottostare a tutte le normative che, nel resto del mondo, nemmeno si sognano.
Di più: fino a che è prodotto da grandi società, è probabile che staff di consulenti e appositi uffici possano anche occuparsi della cosa, ma per il software libero, che a maggior ragione dovrebbe essere... libero, come la mettiamo? Chi si sobbarca oneri di pubblicazione, avvisi e balzelli?

Come ancora Cappato dice nella sua dichiarazione "la Legge Urbani sembra muovere dall'erroneo principio per cui la diffusione di un'opera dell'ingegno debba essere sempre controllata o gestita dall'originario titolare dei diritti, e che al di fuori di tale controllo sia sempre illecita, dimenticando così che la comunicazione e la riproduzione di un'opera in rete sono diritti che l'autore può anche decidere di concedere agli utenti, impiegando una licenza libera quale la GPL per il software o una licenza Creative Commons per le altre opere."

In pratica un pasticcio, che ora è anche una beffa! Attendiamo che vengano ascoltate e approvate le modifiche promesse, tanto sbandierate e per ora ancora sui tavoli di chi le ha proposte.
In definitiva la domanda è poi sempre la stessa: noi utenti possiamo scambiare file in p2p? La legge dice no, ma la pratica, come si vede, è un'altra cosa. ■

Cyberenigma

Quasi tutti hanno scoperto uno dei più bei giochi italiani

LE RISPOSTE

Il gioco era Avventura nel Castello di Enrico Colombini, la prima avventura testuale in italiano, pubblicata nei lontani anni Ottanta. I frammenti di testo erano parte degli aiuti, codificati secondo un semplice cifrario a sostituzione, la cui chiave cambiava per ogni aiuto. Il programma era un Basic di allora che effettuava la decodifica. Avventura nel Castello oggi è freeware, disponibile a http://www.erix.it/avventure.html#freeware.

ISTRUZIONI PER L'USO

1) Rispondere prima che esca il prossimo HJ!
2) Indicare come subject Cyberenigma e possibilmente il numero di riferimento. Per esempio, per questo numero, Cyberenigma 54.
3) Se non è chiaro dalla mail, indicare chiaramente il proprio nickname.
4) Se si manda codice sorgente, meglio che sia nel body della mail piuttosto che in un allegato.

Questo ci aiuterà tantissimo a non perdere nessuno per strada.

GLI AIUTI

CONTENUTO PERGAMENA (25)

Diagnosi: il soggetto pare affetto da grave carenza di senno. Terapia consigliata: due flaconi di furbolina al giorno per sei mesi, e per esercizio scrivere la parola una lettera alla volta.

Diamante (13)

Gli antichi proverbi contengono spesso molta saggezza. In particolare ne contiene quello che trovi nella stanza della principessa.

Parola magica (13)

Hai osservato tutto nella stanza delle colonne? (vedi)

Il codice di Dark_Sun (in mIRC Scripting!)

```
scritto in mIRC Scripting:
nel mirc premi ALT+R ed incolla
Uso:
/cifra codice FRASE
/decifra codice FRASE
Es:
/cifra 20 CIAO
/decifra 13 PUNB
;----------------------
----- Inizio
alias decifra {
 var %x = 1,%r
 while $mid($2-,%x,1) {
  var %a = $asc($ifmatch)
  if (%a = 32) { %r = %r $chr(32) |
goto x }
   if (%a >= 65) { %a = %a + $1 }
   if (%a > 90) { %a  = %a - 26 }
   %r = %r $+ $chr(%a)
   :x | inc %x
  }
 echo -a Decifrato: %r
}
alias cifra {
 var %x = 1,%r
 while $mid($2-,%x,1) {
  var %a = $asc($ifmatch)
  if (%a = 32) { %r = %r $chr(32) |
goto x }
   if (%a >= 65) { %a = $calc(%a -
$1 + 26) }
   if (%a > 90) { %a  = %a - 26 }
   %r = %r $+ $chr(%a)
   :x | inc %x
  }
 echo -a Cifrato: %r
}
```

GLI HACKER DI QUESTO CYBERENIGMA!

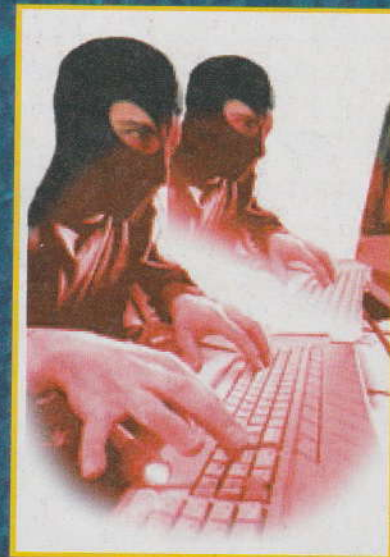
In ordine di arrivo:

AHZRAEL, IL PIÙ VELOCE!
3mentina
ETABETA
KILL4
AlbyRoX
Ransflyer
DiOne
-=[M37h0d]=-
Blink@go
giuseppe
black3y3
Dat@BIT
Dark_Sun
Blade Hook
Devilangel666
Marco
Alessio Failla
Gabriel Popescu
[]Alex[]
Ivoidl
klaus74
Benny

del CASTELLO

prodotto tanto tempo fa, in una galassia lontana lontana

Il codice di Blink@go (Java)

```
public class Passato { public static void main(String[] args)
{
 String Codice = null;
 int cc;
 //il parametro della frase va messo tra doppi apici, altri-
menti ritorna
errore
 try{
  Codice=args[0];
  cc=Integer.parseInt(args[1]);
 }catch(Exception e){
  System.err.println("Insrire come primo parametro la fra-
se e come secondo
la chiave!");
  return;
 }
 StringBuffer sb =new StringBuffer(Codice);
 StringBuffer Risultato=new StringBuffer();

 for(int i=0; i<sb.length(); i++){
  char c=sb.charAt(i);
  if(c>=65){
   c=(char)(c+cc);
   if(c>90){
    c=(char)(c-26);
   }
  }
  Risultato.append(c);
 }
 System.out.println(Risultato.toString());
}
}

//Il codificatore segue lo stesso principio:

public class Codificatore {

public static void main(String[] args) {
 String Codice = null;
 int cc;
 //il parametro della frase va messo tra doppi apici, altri-
menti ritorna
errore
 try{
  Codice=args[0];
  cc=Integer.parseInt(args[1]);
 }catch(Exception e){
  System.err.println("Insrire come primo parametro la fra-
se e come secondo
la chiave!");
  return;
 }

 StringBuffer sb =new StringBuffer(Codice);
        StringBuffer
Risultato=new StringBuf-
fer();
 for(int i=0; i<sb.length();
i++){
  char c=sb.charAt(i);
  if(c>=65){
   c=(char)(c-cc);
   if(c<65){
    c=(char)(c+26);
   }
  }
  Risultato.append(c);
 }

System.out.println(Risul-
tato.toString());
 }
}
```

Pietro Grossi
Sito
Piero da Napoli
Claudio
Irvin "Edward" Dominin
Fabio
Enrico Sunseri
Mordred
domyhck
hack
HARLOK
Daniele Orlando
SuperDario64
Bonny
Andrea Prestigiacomo
Fabio (fabiouz45)
Stefano
rebelsource
yayo.
Carletto
CMOS

Complimenti a tutti e alla prossima!

IL PROSSIMO NUMERO IN EDICOLA IL 15 Luglio 2004!

CYBERENIGMA

Giochi da Hacker!

Una volta si giocava a distanza solo a scacchi, per posta normale (e a suon di lettere una partita durava settimane e costava soldi). Oggi grazie alla Rete si può giocare a distanza a qualsiasi cosa, dalla dama a Dungeons and Dragons o Cyberpunk. Ma c'è un problema: i dadi.

Come si fa lanciare dadi, a estrarre carte, a fidarsi di quello che ti dice chi ti scrive dall'altra parte del mondo? In altre parole, come si fa a disporre di numeri casuali? Un vero dilemma. Ma per fortuna ci sono gli hacker... come noi! La nostra missione è trovare modi ingegnosi per lanciare dadi, ossia generare numeri casuali, usabili in una situazione di gioco a distanza.

Regole: casuale significa che il giocatore non ha modo di sapere con certezza che cosa uscirà e non può barare sfruttando la conoscenza del meccanismo.
Si presuppone che i giocatori comunichino solo via Internet.
Non valgono meccanismi che impongono comunicazione sincrona (chat, videoconferenze o altri sistemi in cui c'è connessione diretta e contemporanea tra giocatori). Il meccanismo deve poter funzionare senza comunicazioni in tempo reale.

✪ **Per tutti:** Trovare su Internet un modo per lanciare dadi da usare nel gioco a distanza.
✪✪ **Per esperti:** Trovare un modo fuori dal web per lanciare dadi da usare nel gioco a distanza. I più bravi riusciranno a pensare a uno o più modi per lanciare dadi senza usare computer. I più bravi ancora penseranno a un meccanismo di controllo e verifica dei lanci, in modo che nessuno possa barare. Più semplice è il meccanismo, meglio è.
✪✪✪ **Per geni:** Programmare un meccanismo di lancio di dadi che sia veramente casuale, alla luce di un test di almeno un migliaio di lanci.
✪✪✪✪ **Per super hacker:** Pensare ed eventualmente programmare un meccanismo che consenta a due o più persone di giocare a distanza a carte (qualunque gioco, da briscola a Magic). I più bravi (ma bravi proprio) riusciranno a farlo senza passare da un server centrale.

Alla prossima!

le risposte a:

guestbook@hackerjournal.it